Exhibit C

Attorney Docket No: 8906P001F4 Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application:

First Named Inventor:

Lee Hahn Holloway

Application No. 12/939,926

Filed: 11/04/2010

For: INTERNET-BASED PROXY SERVICE TO MODIFY INTERNET RESPONSES

Examiner: Hillery, Nathan

Art Unit: 3715

Confirmation No: 6414

EFS Filing
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

Sir:

In response to the Office Action dated January 14, 2015, please amend the above-identified application as follows and consider the following remarks.

IN THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Previously Presented) A method in a proxy server to modify Internet responses, comprising:

receiving, at the proxy server from a client device, a request for a network resource that is hosted at an origin server for a domain, wherein the request is received at the proxy server as a result of a DNS (Domain Name System) request for the domain returning an IP address of the proxy server instead of an IP address of the origin server, and wherein the origin server is one of a plurality of origin servers that belong to different domains that resolve to the proxy server and are owned by different entities;

retrieving, by the proxy server, the requested network resource;

determining, by the proxy server, that the requested network resource is an HTML (HyperText Markup Language) page;

scanning, by the proxy server, the HTML page to locate one or more modification tokens, wherein each modification token indicates content that is subject to being modified;

for at least one located modification token, automatically modifying, by the proxy server, at least a portion of the content of the HTML page that corresponds to that modification token; and

transmitting, by the proxy server, the modified HTML page to the client device.

2. (Previously Presented) The method of claim 1, wherein retrieving, by the proxy server, the requested network resource includes performing the following:

determining whether the requested network resource is available in cache;

responsive to a determination that the requested network resource is not available in cache, performing the following:

transmitting the request to the origin server, and receiving the network resource from the origin server; and

responsive to a determination that the requested network resource is available in cache, accessing the cache to retrieve the requested network resource.

3. (Previously Presented) The method of claim 1, wherein the HTML page includes at least one obfuscation modification token that identifies an element to be obfuscated, wherein the at least one located modification token is the at least one obfuscation modification token, and wherein automatically modifying, by the proxy server, at least [[a]] the portion of the HTML content corresponding to that obfuscation modification token includes performing the following:

automatically replacing at least the element to be obfuscated of the HTML content that corresponds to the obfuscation modification token with an obfuscation script, which when executed by a client network application of the client device, generates the element such that it will be displayed on the rendered HTML page while not being directly readable by bots that scan a source of the HTML page.

4. (Original) The method of claim 3, wherein the element to be obfuscated is one of: a phone number, an email address, an instant messenger identifier, a street address, a link to another website, a birthdate, a social security number, an IP address, a credit card number, and an account username.

5. (Original) The method of claim 3, wherein the element to obfuscated is an email address, and wherein the obfuscation script generates the email address to be displayed in the rendered HTML page and is not readable in the page source of the HTML page, and the obfuscation script further encodes the email address with a mailto attribute such that when selected a new email message will be created that is addressed to that email address.

6. (Previously Presented) The method of claim 1, wherein the HTML page includes at least one modification token that is a server side defined modification (SSDM) token that is defined by an administrator of the domain and indicates that content is subject to being one of excluded and obfuscated; and wherein the at least one located modification

token is the SSDM token.

7. (Original) The method of claim 6, wherein the SSDM token is defined with a set of one or more modification rules that specify the conditions on which the content is to be excluded or obfuscated based on one or more characteristics associated with the request.

8. (Previously Presented) The method of claim 6, wherein the SSDM token indicates that an element is subject to being obfuscated, and wherein automatically modifying, by the proxy server, at least a portion of the HTML content corresponding to the SSDM token includes performing the following:

automatically replacing at least the element to be obfuscated of the HTML content that corresponds to the SSDM token with an obfuscation script, which when executed by a client network application of the client device, generates the element such that it will be displayed on the rendered HTML page while not being directly readable by bots that scan a source of the HTML page.

9. (Previously Presented) The method of claim 6, wherein the SSDM token indicates that an element is subject to being excluded from the HTML page, and wherein automatically modifying, by the proxy server, at least a portion of the HTML content corresponding to the SSDM token includes automatically removing at least a portion of the HTML content represented by the SSDM token.

10. (Previously Presented) A proxy server to modify Internet responses, comprising:

a memory to store instructions;

a processor coupled with the memory to process the stored instructions to

receive, from a client device, a request for a network resource that is hosted at an origin server for a domain, wherein the request is received at the proxy server as a result of a DNS (Domain Name System) request for the domain returning an IP address of the proxy server instead of an IP address of the origin server, and wherein the origin server is one of a plurality of origin servers that belong to different domains that resolve to the proxy server and are owned by different entities;

retrieve the requested network resource;

determine that the requested network resource is an HTML (HyperText Markup Language) page;

scan the HTML page to locate one or more modification tokens, wherein each modification token indicates content that is subject to being modified;

for at least one located modification token, automatically modify at least a portion of the content of the HTML page that corresponds to that modification token; and

transmit the modified HTML page to the client device.

11. (Original) The proxy server of claim 10, wherein retrieval of the requested network resource includes the processor to process the stored instructions to perform the following:

determine whether the requested network resource is available in cache;

responsive to a determination that the requested network resource is not available in cache, perform the following:

transmit the request to the origin server, and

receive the network resource from the origin server; and

responsive to a determination that the requested network resource is available in cache, access the cache to retrieve the requested network resource.

12. (Original) The proxy server of claim 10, wherein the HTML page includes at least one obfuscation modification token that identifies an element to be obfuscated, and wherein the automatic modification of at least a portion of the HTML content corresponding to that obfuscation modification token includes the processor to process the stored instructions to perform the following:

automatically replace at least the element to be obfuscated of the HTML content that corresponds to the obfuscation modification token with an obfuscation script, which when executed by a client network application of the client device, generates the element such that it will be displayed on the rendered HTML page while not being directly readable by bots that scan a source of the HTML page.

13. (Original) The proxy server of claim 12, wherein the element to be obfuscated is one of: a phone number, an email address, an instant messenger identifier, a street address, a link to another website, a birthdate, a social security number, an IP address, a credit card number, and an account username.

14. (Original) The proxy server of claim 12, wherein the element to obfuscated is an email address, and wherein the obfuscation script generates the email address to be displayed in the rendered HTML page and is not readable in the page source of the HTML page, and the obfuscation script further encodes the email address with a mailto attribute such that when selected a new email message will be created that is addressed to that email address.

15. (Original) The proxy server of claim 10, wherein the HTML page includes at least one modification token that is a server side defined modification (SSDM) token that is defined by an administrator of the domain and indicates that content is subject to being one of excluded and obfuscated.

16. (Original) The proxy server of claim 15, wherein the SSDM token is defined with a set of one or more modification rules that specify the conditions on which the content is to be excluded or obfuscated based on one or more characteristics associated with the request.

17. (Original) The proxy server of claim 15, wherein the SSDM token indicates that an element is subject to being obfuscated, and wherein automatic modification of at least a portion of the HTML content corresponding to the SSDM token includes the processor to process the stored instructions to perform the following:

automatically replace at least the element to be obfuscated of the HTML content that corresponds to the SSDM token with an obfuscation script, which when executed by a client network application of the client device, generates the element such that it will be displayed on the rendered HTML page while not being directly readable by bots that scan a source of the HTML page.

18. (Original) The proxy server of claim 15, wherein the SSDM token indicates that an element is subject to being excluded from the HTML page, and wherein automatic modification of at least a portion of the HTML content corresponding to the SSDM token includes the processor to process the stored instructions to automatically remove at least a portion of the HTML content represented by the SSDM token.

19. (Previously Presented) A non-transitory machine-readable storage medium that provides instructions that, when executed by a processor of a proxy server, cause said processor to perform operations comprising:

receiving, from a client device, a request for a network resource that is hosted at an origin server for a domain, wherein the request is received at the proxy server as a result of a DNS (Domain Name System) request for the domain returning an IP address of the proxy server instead of an IP address of the origin server, and wherein the origin server is one of a plurality of origin servers that belong to different domains that resolve to the proxy server and are owned by different entities;

retrieving the requested network resource;

determining that the requested network resource is an HTML (HyperText Markup Language) page;

scanning the HTML page to locate one or more modification tokens, wherein each modification token indicates content that is subject to being modified;

for at least one located modification token, automatically modifying at least a portion of the content of the HTML page that corresponds to that modification token; and

transmitting the modified HTML page to the client device.

20. (Original) The non-transitory machine-readable storage medium of claim 19, wherein retrieving the requested network resource includes performing the following:

determining whether the requested network resource is available in cache;

responsive to a determination that the requested network resource is not available in cache, performing the following:

transmitting the request to the origin server, and receiving the network resource from the origin server; and

responsive to a determination that the requested network resource is available in cache, accessing the cache to retrieve the requested network resource.

21. (Original) The non-transitory machine-readable storage medium of claim 19, wherein the HTML page includes at least one obfuscation modification token that identifies an element to be obfuscated, and wherein automatically modifying at least a portion of the HTML content corresponding to that obfuscation modification token includes performing the following:

automatically replacing at least the element to be obfuscated of the HTML content that corresponds to the obfuscation modification token with an obfuscation script, which when executed by a client network application of the client device, generates the element such that it will be displayed on the rendered HTML page while not being directly readable by bots that scan a source of the HTML page.

22. (Original) The non-transitory machine-readable storage medium of claim 21, wherein the element to be obfuscated is one of: a phone number, an email address, an instant messenger identifier, a street address, a link to another website, a birthdate, a social security number, an IP address, a credit card number, and an account username.

23. (Original) The non-transitory machine-readable storage medium of claim 21, wherein the element to obfuscated is an email address, and wherein the obfuscation script generates the email address to be displayed in the rendered HTML page and is not readable in the page source of the HTML page, and the obfuscation script further encodes the email address with a mailto attribute such that when selected a new email message will be created that is addressed to that email address.

24. (Original) The non-transitory machine-readable storage medium of claim 19, wherein the HTML page includes at least one modification token that is a server side defined modification (SSDM) token that is defined by an administrator of the domain and indicates that content is subject to being one of excluded and obfuscated.

25. (Original) The non-transitory machine-readable storage medium of claim 24, wherein the SSDM token is defined with a set of one or more modification rules that specify the conditions on which the content is to be excluded or obfuscated based on one or more characteristics associated with the request.

26. (Original) The non-transitory machine-readable storage medium of claim 24, wherein the SSDM token indicates that an element is subject to being obfuscated, and wherein automatically modifying at least a portion of the HTML content corresponding to the SSDM token includes performing the following:

automatically replacing at least the element to be obfuscated of the HTML content that corresponds to the SSDM token with an obfuscation script, which when executed by a client network application of the client device, generates the element such that it will be displayed on the rendered HTML page while not being directly readable by bots that scan a source of the HTML page.

27. (Original) The non-transitory machine-readable storage medium of claim 24, wherein the SSDM token indicates that an element is subject to being excluded from the HTML page, and wherein modifying at least a portion of the HTML content corresponding to the SSDM token includes automatically removing at least a portion of the HTML content represented by the SSDM token.

28. (Previously Presented) The method of claim 1, wherein the at least one located modification token indicates content that is potentially a threat to a visitor, and wherein automatically modifying, by the proxy server, at least the portion of the HTML content corresponding to that modification token includes removing that portion of the HTML content.

29. (Previously Presented) The proxy server of claim 10, wherein the at least one located modification token indicates content that is potentially a threat to a visitor, and wherein the automatic modification of at least the portion of the HTML content corresponding to that modification token includes the processor to process the stored instructions to remove that portion of the HTML content.

30. (Previously Presented) The non-transitory machine-readable storage medium of claim 19, wherein the at least one located modification token indicates content that is potentially a threat to a visitor, and wherein automatically modifying, by the proxy server, at least the portion of the HTML content corresponding to that modification token includes removing that portion of the HTML content.

REMARKS

The enclosed is responsive to the Examiner's Office Action mailed on January 14, 2015. At the time the Examiner mailed the Office Action, claims 1-30 were pending. By way of the present response applicants have: 1) amended no claims; 2) added no claims; and 3) canceled no claims. No new matter has been added. Reconsideration of this application as amended is respectfully requested.

Claim Rejections – 35 U.S.C. § 101

Claims 1-30 stand rejected under 35 U.S.C. § 101 because the claimed invention is allegedly directed to non-statutory subject matter.

The Office Action states that the "claim(s) is/are directed to the abstract idea of modifying internet responses" and that "additional claim element(s) do not provide meaningful limitation(s) to transform the abstract idea into a patent eligible application of the abstract idea such that the claim(s) amounts to significantly more than the abstract idea itself." Office Action, Page 3. Applicant respectfully disagrees.

First, Applicant respectfully submits that claims 1-30 are not directed to an abstract idea. As provided in the Abstract Ideas Examples document that accompanies the 2014 Interim Guidance (located here: http://www.uspto.gov/patents/law/exam/abstract_idea_examples.pdf), there are several examples of what is not an abstract idea. For instance, Example 1 is a method for isolating and removing malicious code from electronic messages, which is not an abstract idea. As another example, Example 2 is an e-commerce outsourcing system/generating a composite web page, which is not an abstract idea. As detailed in the discussion of Example 2, the invention differed from other claims found by the courts to recite abstract ideas in that it did not "merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet. Instead, the claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks." *See* pages 4-5 of the Abstract Ideas Examples document, citing *DDR Holdings, LLC v. Hotels.com et al.*, 113 USPQ2d 1097 (Fed. Cir. 2014).

Here, claims 1-30 are not directed to an abstract idea. As similarly found by the Federal Circuit with respect to *DDR Holdings*, claims 1-30 do not "merely recite the performance of some business practice known from the pre-Internet world along with the requirement to perform it on the Internet." Instead, claims 1-30 is necessarily rooted in computer technology arising in the realm of computer networking. Claims 1-30 do not describe a fundamental economic practice, a method of organizing human activity, an idea itself (standing alone), or a mathematical relationship. Accordingly, claims 1-30 do not recite an abstract idea and therefore are not directed to any judicial exception.

Since claims 1-30 are not directed to an abstract idea, Applicant respectfully submits that there is no need for the second step of the *Alice* analysis and claims 1-30 are patent eligible.

Claim Rejections – 35 U.S.C. § 103

Claims 1, 2, 10, 11, 19, 20, and 28-30 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2006/0288119 A1 by Kim et al. (hereinafter, "Kim") in further view of U.S. Patent Publication No. 2010/0076851 A1 by Jewell (hereinafter, "Jewell"), U.S. Patent Publication No. 2010/0169465 A1 by Amidon et al. (hereinafter, "Amidon"), and U.S. Patent Publication No. 2005/0267869 A1 by Horvitz et al. (hereinafter, "Horvitz"). Claims 3, 4, 12, 13, 21, and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kim, Jewell, Amidon and Horvitz as applied to claims 1, 10, and 19, and further in view of U.S. Patent Publication No. 2009/0300206 A1 by Todorov (hereinafter, "Todorov"). Claims 5, 14, and 23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kim, Jewell, Amidon, Horvitz and Todorov as applied to claims 3, 12, and 21, and further in view of U.S. Patent Publication No. 2005/0114453 A1 by Hardt (hereinafter, "Hardt"). Claims 6, 7, 15, 16, 24, and 25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kim, Jewell, Amidon, and Horvitz as applied to claims 1, 10, and 19, and further in view of Hardt. Claims 8, 9, 17, 18, 26, and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kim, Jewell, Amidon, Horvitz and Hardt as applied to claims 6, 15, and 24, and further in view of Todorov. Applicant respectfully traverses.

Claim 1

Applicant respectfully submits that claim 1 is not obvious over Kim in view of Jewell in further in view of Amidon and in further in view of Horvitz for at least the reason that the proposed combination does not teach or suggest each limitation of claim 1.

Applicant respectfully submits that the proposed combination of Kim, Jewell, Amidon, and Horvitz does not teach or suggest "*for at least one located modification token, automatically modifying, by the proxy server, at least a portion of the content of the HTML page that corresponds to that modification token*" as required by claim 1. In considering this limitation, the Office Action correctly acknowledges that none of Kim, Jewell, and Amidon teach or suggest this limitation.[1] However, the Office Action cites paragraph 73 of Horvitz as allegedly teaching this limitation. Applicant respectfully disagrees that cited paragraph 73 of Horvitz teaches this limitation.

Paragraph 73 of Horvitz describes a process for collecting data and mining models. A user directs their web browser through a proxy that logs data requests. Before mining user or collaborative access patterns, the logged data is cleaned, which includes removing data requests for embedded content by parsing the HTML of requested pages and identifying which URLs are embedded. However, paragraph 73 of Horvitz does not disclose "*for at least one located modification token, automatically modifying, by the proxy server, at least a portion of the content of the HTML page that corresponds to that modification token*" as required by claim 1. Although Horvitz discloses cleaning a data request log by removing requests for embedded content, a data request log is not the HTML page itself. Thus, Horvitz does not teach "*for at least one located modification token, automatically modifying, by the proxy server, at least a portion of the content of the HTML page that corresponds to that modification token*" as required by claim 1.

Therefore, for at least the above reason, Applicant respectfully submits that claim 1 is not obvious in view of Kim, Jewell, Amidon, and Horvitz. Since claims 10 and 19 include similar limitations as claim 1, Applicants respectfully submit that they are also not obvious in view of Kim, Jewell, Amidon, and Horvitz for at least similar reasons. Since claims 2, 11, 20, and 28-30 are dependent claims, Applicants respectfully submit that they are not obvious in view of Kim and Jewell for at least similar reasons.

Other Dependent Claims

Applicants respectfully submit that claims 3, 4, 12, 13, 21, and 22 are not obvious over Kim, Jewell, Amidon, Horvitz, and further in view of Todorov for at least the reason that they depend on an allowable claim. Applicants respectfully submit that claims 5, 14, and 23 are not obvious over Kim, Jewell, Amidon, Horvitz, Todorov, and further in view of Hardt for at least the reason that they depend on an allowable claim. Applicants respectfully submit that claims 6, 7, 15, 16, 24, and 25 are not obvious over Kim, Jewell, Amidon, Horvitz and further in view of Hardt for at least the reason that they depend on an allowable claim. Applicants respectfully submit that claims 8, 9, 17, 18, 26, and 27 are not obvious over Kim, Jewell, Amidon, Horvitz, Hardt, and further in view of Todorov for at least the reason that they depend on an allowable claim.

[1] The Office Action states that Horvitz does not teach this limitation; however Applicant assumes this is a typographical error and that the Office Action meant to state that Amidon does not teach this limitation.

CONCLUSION

Applicant respectfully submits that in view of the amendments and arguments set forth herein, the applicable objections and rejections have been overcome. To the extent that Applicant has not addressed a specific claim element alleged by the Office Action to be covered by prior art, or any other reason for rejection, should not be viewed as an admission that the Applicant accepts or agrees with the Office Action's reasoning and Applicant reserves the right of argument in a future response. Accordingly, Applicant respectfully requests reconsideration and withdrawal of the claim rejections. Applicant reserves all rights under the doctrine of equivalents.

Pursuant to 37 C.F.R. 1.136(a)(3), Applicant hereby requests and authorizes the U.S. Patent and Trademark Office to (1) treat any concurrent or future reply that requires a petition for extension of time as incorporating a petition for extension of time for the appropriate length of time and (2) charge all required fees, including extension of time fees and fees under 37 C.F.R. 1.16 and 1.17, to Deposit Account No. 506674.

Respectfully submitted,

Nicholson De Vos Webster & Elliott LLP

Date: June 15, 2015

/Matthew N. Nicholson/
Matthew N. Nicholson
Reg. No. 62, 889